JOURNAL OF COMBINATORIAL THEORY (A) 13, 422–425 (1972)

NOTE

A Simplification of Moore's Proof of the Existence of Steiner Triple Systems

A. J. W. HILTON

Department of Mathematics, University of Reading, Reading, England

Communicated by N. G. de Bruijn

Received April 7, 1971

1. INTRODUCTION

A Steiner triple system of order $v \geqslant 1$ is a set of triples of elements from a set A of v elements such that each pair of elements of A is in exactly one triple. We denote such a system by $S(A)$. It is easy to see that a necessary condition for the existence of a Steiner triple system of order v is that $v \equiv 1$ or 3 (mod 6). (There are trivial systems when $v = 1$ or 3.) The most widely known proof of the sufficiency of this condition, (given in Netto's book "Lehrbuch der Combinatorik" and in Marshall Hall's book, "Combinatorial Theory") was due to Moore [4] in 1893. For a recent direct construction, see [3], and for a comprehensive list of references, see [1]. Moore's method, a recursive one, involves constructing a Steiner triple system with a subsystem of order 7 for almost all orders. In this note we simplify the proof by avoiding the necessity of constructing Steiner triple systems with subsystems of order 7.

2. CONSTRUCTIONS

Two constructions used by Moore are also used here:

First, let $S(A)$ and $S(B)$ be two Steiner triple systems of orders v_1 and v_2, respectively. Let $S(A) \times S(B)$ denote the Steiner triple system of order $v_1 v_2$ whose triples are

(i) $\{(a_i, b_r), (a_j, b_r), (a_k, b_r)\}$ for all $b_r \in B$, $\{a_i, a_j, a_k\} \in S(A)$,

(ii) $\{(a_i, b_r), (a_i, b_s), (a_i, b_t)\}$ for all $a_i \in A$, $\{b_r, b_s, b_t\} \in S(B)$,

(iii) $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\}$ for all $\{a_i, a_j, a_k\} \in S(A)$, $\{b_r, b_s, b_t\} \in S(B)$.

Note that, if $\{a_i, a_j, a_k\} \in S(A)$ and $\{b_r, b_s, b_t\} \in S(B)$, then $S(A) \times S(B)$ includes $S(\{a_i, a_j, a_k\}) \times S(\{b_r, b_s, b_t\})$ as a subsystem. Therefore, if there is a system of order $\nu_1 \geqslant 3$ and one of order $\nu_2 \geqslant 7$, then there is one of order $\nu_1\nu_2$ with a subsystem of order 9.

Second, let $S(A')$, $S(A)$ and $S(B)$ be three Steiner triple systems of orders ν_3, ν_2, and ν_1, respectively, with $A' \subset A$, $A \backslash A' = [1, 2, \ldots, \nu_2 - \nu_3]$, and $\nu_1 \geqslant 3$. Then there is a Steiner triple system of order $\nu_3 + \nu_1(\nu_2 - \nu_3)$ whose triples are

(i) $\{a_i, a_j, a_k\}$ for all $\{a_i, a_j, a_k\} \in S(A')$,

(ii) $\{a_i, (a_j, b_r), (a_k, b_r)\}$ for all $\{a_i, a_j, a_k\} \in S(A)$ with $a_i \in A'$, $a_j, a_k \in A \backslash A'$, and for all $b_r \in B$,

(iii) $\{(a_i, b_r), (a_j, b_r), (a_k, b_r)\}$ for all $\{a_i, a_j, a_k\} \in S(A)$ with $a_i, a_j, a_k \in A \backslash A'$ and for all $b_r \in B$,

(iv) $\{(a_i, b_r), (a_j, b_s), (a_k, b_t)\}$ for all a_i, a_j, a_k such that $a_i + a_j + a_k \equiv 0 \pmod{\nu_2 - \nu_3}$ and all $\{b_r, b_s, b_t\} \in S(B)$.

The only values of ν_3 we shall use are 1, 3, and 9, but, of course, ν_3 need not be restricted to these values.

3. Recursive Construction for All Orders

First, we need an example of a Steiner triple system of order 13. This is provided by the triples

$$\{x, x+1, x+4\}, \qquad \{x, x+2, x+7\} \qquad (x = 1, 2, \ldots, 13),$$

the numbers being taken modulo 13.

Next we note that systems of order up to 36 may be constructed as follows, writing each order in the form $\nu_1\nu_2$ or $\nu_3 + \nu_1(\nu_2 - \nu_3)$ to suggest the parameters in the constructions described in Section 2:

1, trival, 3, trivial, $7 = 1 + 3(3-1)$, $9 = 3 \times 3$, 13 above,

$15 = 1 + 7(3-1)$, $19 = 1 + 9(3-1)$, $21 = 3 \times 7$,

$25 = 1 + 3(9-1)$, $27 = 3 \times 9$, $31 = 1 + 15(3-1)$, $33 = 3 + 3(13-3)$.

Systems of higher order may now be constructed recursively in view of the following equalities:

$$
\begin{aligned}
36t + 1 &= 1 + 3(\overline{12t + 1} - 1),\\
36t + 3 &= 1 + (18t + 1)(3 - 1),\\
36t + 7 &= 1 + (6t + 1)(7 - 1),\\
36t + 9 &= 3 + (6t + 1)(9 - 3),\\
36t + 13, &\qquad \text{see below},\\
36t + 15 &= 1 + (18t + 7)(3 - 1),\\
36t + 19 &= 1 + (6t + 3)(7 - 1),\\
36t + 21 &= 3 + (6t + 3)(9 - 3),\\
36t + 25 &= 1 + 3(\overline{12t + 9} - 1),\\
36t + 27 &= 1 + (18t + 13)(3 - 1),\\
36t + 31 &= 1 + (18t + 15)(3 - 1),\\
36t + 33 &= 3 + 3(\overline{12t + 13} - 3).
\end{aligned}
$$

Systems of order $36t + 13$ may be formed as follows: The number $36t + 13$ may be re-expressed

$$
\begin{aligned}
36t + 13 &= 1 + (3t + 1)\,3.2^2\\
&= 1 + (3[2^0 + 2^2 + 2^4 + \cdots + 2^{2r-2} + 2^{2r+\alpha_0} + \cdots + 2^{2r+\alpha_s}] + 1)\,3.2^2
\end{aligned}
$$

for some integers $r, \alpha_0, \alpha_1, \ldots, \alpha_s$, where $r \geqslant 0$ and $0 < \alpha_0 < \alpha_1 < \cdots < \alpha_s$,

$$
= 1 + (3x + 1)\,3.2^{2r+2},
$$

where $x \equiv 0, 2$, or $3 \pmod 4$. Therefore, for some integer $n \geqslant 0$,

$$
36t + 13 = \begin{cases} 1 + (6n + 1)([3.2^{2r+2} + 1] - 1), \\ \text{or} \quad 1 + (18n + 15)([2^{2r+3} + 1] - 1). \end{cases}
$$

This provides a construction unless $36t + 13 = 1 + 3.2^{2r+2}$, in which case $t = 2^{2r-2} + \cdots + 2^2 + 2^0$. When $r = 2s + 2$, $s \geqslant 0$, we have

$$
\begin{aligned}
36t + 13 &= 36[2^{4s+2} + 2^{4s} + \cdots + 2^0] + 13\\
&= 36[2^{4s} + 2^{4s-4} + \cdots + 2^0][2^2 + 2^0] + 13\\
&= 3 + (18[2^{4s} + 2^{4s-4} + \cdots + 2^0] + 1)(13 - 3).
\end{aligned}
$$

When $r = 2s + 3$, $s \geqslant 0$, we have

$$\begin{aligned} 36t + 13 &= 36[2^{4s+4} + 2^{4s} + \cdots + 2^0] + 13 \\ &= 36([2^{4s+2} + 2^{4s-2} + \cdots + 2^2][2^2 + 2^0] + 2^0) + 13 \\ &= 18[2^{4s} + 2^{4s-4} + \cdots + 2^0]\,40 + 49 \\ &= 9 + (18[2^{4s} + 2^{4s-4} + \cdots + 2^0] + 1)(49 - 9). \end{aligned}$$

Finally, when $r = 1$ we have $t = 1$ and so $36t + 13 = 49 = 7 \times 7$.

References

1. J. Doyen, Sur la croissance du nombre de systèmes triples de Steiner non isomorphes, *J. Combinatorial Theory* **8** (1970), 424–441.
2. M. Hall, Jr., "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
3. A. J. W. Hilton, On Steiner and similar triple systems, *Math. Scand.* **24** (1969), 208–216.
4. E. H. Moore, Concerning Triple Systems, *Math. Ann.* **43** (1893), 271–285.
5. E. Netto, "Lehrbuch der Combinatorik," 2nd ed. (Erweitert und mit Anmerkungen versehen von V. Brun und Th. Skolem, Berlin, 1927); reprinted by Chelsea, New York, 1958.